WHAT IS CLAIMED IS:

1. A data library system with managed device access, said system comprising:

at least one partition;

a plurality of data transfer elements each of said data transfer elements assigned to a partition;

a plurality of data storage element slots, each of said slots assigned to a partition;

a library controller comprising a virtual controller for each partition, said virtual controller directing movement of said media to and from said slots assigned to a same partition and to and from said data transfer elements assigned to said same partition; and

at least one bridge operatively disposed between at least one user and said library, each of said bridges present said data transfer elements and said virtual controllers of each partition to said users as logical components beginning at a same designation for each partition.

2. The system of claim 1 wherein at least one of said at least one partition is secured and access to a particular one of said at least one secured partition is restricted to said users having a unique host device identifier listed in a list of unique host device identifiers for access to said particular partition.

3. The system of claim 2 wherein said list of unique host device identifiers is maintained on said at least one bridge.

4. The system of claim 1 wherein said at least one bridge is a fiber channel to small computer systems interface bridge.

5. The system of claim 2 wherein said unique host device identifiers are world wide names.

6. The system of claim 2 wherein said unique host device identifiers are iSCSI names.

7. The system of claim 1 wherein said logical element designations are fiber channel logical unit numbers.

8. A data library bridge adapted to be operatively disposed between at least one user and said data library, said bridge comprising:

means for presenting data transfer elements of said data library attached to said bridge as logical units; and

means for presenting a controller for each partition of said data library as a logical unit, said controller directing movement of media to and from storage element slots of said library assigned to a library partition to and from said data transfer elements assigned to a same partition;

wherein designations for said logical units in each partition begin at a same number for each partition.

9. The bridge of claim 8 further comprising:

means for listing unique host device identifiers allowed to access a particular partition; and

means for securing selected ones of said partitions by limiting access to said particular partition to said users having a unique host device identifier listed by said means for listing.

10. The bridge of claim 8 wherein said bridge further comprises means for providing a network interface using fiber channel protocols.

11. The bridge of claim 10 wherein said bridge further comprises means for providing a library interface using small computer systems interface protocols .

12. A method for partitioning and managing a data library adapted to be attached to a storage area network, said method comprising:

establishing a plurality of partitions in said data library, each of said partitions comprising at least one storage element slot and at least one data transfer element;

controlling movement of media to and from said slots to and from said data transfer elements assigned to a same partition; and

presenting virtual controllers and said data transfer elements for each of said partitions to users of said library as logical components beginning at a same designation for each of said partitions.

13. The method of claim 12 further comprising:

securing selected ones of said partitions by assigning a list of unique host device identifiers which may access each of said partitions.

14. The method of claim 13 further comprising:

maintaining said list of unique host device identifiers in at least one bridge disposed between said data library and said users.

15. The method of claim 12 wherein said presenting is carried out by at least one bridge disposed between said data library and said users.

16. The method of claim 13 further comprising:

entering security settings for one of said partitions.

17. The method of claim 16 wherein said entering comprises:

listing at least one unique host device identifier authorized to access said one partition.

18. The method of claim 16 wherein said entering comprises:

determining at least one bridge affected by said security settings;

19. The method of claim 16 wherein said entering comprises:

sending said security setting for said one partition to said at least one affected bridge.

20. The method of claim 16 wherein said entering comprises:

adding said security settings to a security lookup-table maintained by at least one affected bridge.

21. The method of claim 16 wherein said security settings comprise a list of virtual unit designations of at least one of said data transfer elements and said virtual controllers of said one partition attached to at least one affected bridge.

22. The method of claim 21 wherein said adding step further comprises:

removing all data transfer element and virtual controller designations from said look-up table for said one partition.

23. The method of claim 21 wherein said adding step further comprises:

adding listed data transfer elements and virtual controllers to an unsecured row of said table in response to said settings comprising an unsecure command.

24. The method of claim 21 wherein said adding step further comprises:

matching unique host device identifiers listed in said settings to existing look up table entries.

25. The method of claim 21 wherein said adding step further comprises:

adding unmatched unique host device identifiers to said table with listed data transfer elements and virtual controllers for said one partition.

26. The method of claim 25 wherein said adding step further comprises:

adding listed data transfer elements and virtual controllers for said one partition to table entries for matched unique host device identifiers.

27. The method of claim 12 wherein said logical element designations are fiber channel logical unit numbers.

28. A partitioned storage area network with a managed attached data library, said network comprising:

a data storage array divided into partitions;

at least one bridge disposed between said array and said library; and

said library comprising:

a plurality of library partitions corresponding to said array partitions;

a plurality of data transfer elements each of said data transfer elements assigned to one of said library partitions;

a plurality of data storage element slots, each of said slots assigned to one of said library partitions; and

a library controller that defines a virtual controller for each of said library partitions, each of said virtual controllers directing movement of said media to and from said slots assigned to a same partition and to and from said data transfer elements assigned to said same partition;

wherein said at least one bridge presents said data transfer elements and said virtual controllers of each of said partitions to users of said network as logical unit numbers beginning at a same logical unit number within each partition.

29. The network of claim 28 wherein a particular one of said partitions is secured at least in part by assigning a list of unique host device identifiers which may access said particular partition.

30. The network of claim 29 wherein said list of unique host device identifiers is maintained on said at least one bridge.

31. The network of claim 29 wherein said unique host device identifiers are world wide names.

32. The network of claim 28 wherein said unique host device identifiers are iSCSI names.

33. The network of claim 28 wherein data mover interconnectivity extends between said array and said library, via said at least one bridge, and said data mover interconnectivity is partitioned and assigned to said corresponding library and array partitions.

34. The network of claim 28 wherein said at least one bridge is a fiber channel to small computer networks interface bridge.